



BOAF / AIA-FLORIDA / FES JOINT TASK FORCE

DIGITAL SIGNATURES

CREATING AND VALIDATING SECURE ELECTRONIC DOCUMENTS

SECURING ELECTRONIC DOCUMENTS

- ▶ Digital signatures can be used by design professionals (Architects and Engineers) to authenticate the electronic documents they create for submittal to a permitting authority.
- ▶ This method of authenticating documents is authorized by the respective licensing boards by Administrative Rule
- ▶ Architects 61G1-16.005
- ▶ Engineers 61G15-23.003

61G1-16.005

- ▶ **61G1-16.005 Procedures for Signing and Sealing Electronically Transmitted Plans, Specifications, Reports or Other Documents.**
- ▶ (1) Information stored in electronic files representing plans, specifications, plats, reports, or other documents which must be sealed under the provisions of Chapter 481, F.S., shall be signed, dated and sealed by the architect or interior designer in responsible charge.
- ▶ (a) A scanned image of an original signature shall not be used in lieu of a digital or electronic signature.
- ▶ (b) The date that the electronic signature file was created or the digital signature was placed into the document must appear on the document in the same manner as date is required to be applied when a licensee uses the manual sealing procedure set out in Rule 61G1-16.003, F.A.C.

61G1-16.005

- ▶ (2) An architect or interior designer utilizing a digital signature to seal construction documents shall assure that the digital signature is:
 - ▶ (a) Unique to the person using it;
 - ▶ (b) Capable of verification;
 - ▶ (c) Under the sole control of the person using it; and
 - ▶ (d) Linked to a document in such a manner that the electronic signature is invalidated if any data in the document are changed.

61G15-23.003

- ▶ **61G15-23.003 Procedures for Signing and Sealing Electronically Transmitted Plans, Specifications, Reports or Other Documents.**
- ▶ (1) Engineering work which must be sealed under the provisions of Section 471.025, F.S., may be signed electronically or digitally as provided herein by the professional engineer in responsible charge. As used herein, the terms “digital signature” and “electronic signature” shall have the meanings ascribed to them in Sections 668.003(3) and (4), F.S. The affixing of a digital or electronic signature to engineering work as provided herein shall constitute the sealing of such work.
- ▶ (a) A scanned image of an original signature shall not be used in lieu of a digital or electronic signature.
- ▶ (b) The date that the electronic signature file was created or the digital signature was placed into the document must appear on the document in the same manner as date is required to be applied when a licensee uses the manual sealing procedure set out in Rule 61G15-23.002, F.A.C.

61G15-23.003

- ▶ (2) A professional engineer utilizing a digital signature to seal engineering work shall assure that the digital signature is:
 - ▶ (a) Unique to the person using it;
 - ▶ (b) Capable of verification;
 - ▶ (c) Under the sole control of the person using it;
 - ▶ (d) Linked to a document in such a manner that the electronic signature is invalidated if any data in the document are changed.

DIGITAL SIGNATURES

- ▶ A key point to remember is that a digital signature is only valid when the associated electronic document (digital file) can be authenticated with the signee's public key
- ▶ A paper printout of a digitally signed electronic document cannot be validated, and therefore cannot be used as an official record
- ▶ A digital signature must be created using key pair technology in accordance with the federal Secure Hash Standard also known as Federal Information Processing Standards, FIPS 180-3 or FIPS 180-4

HOW DIGITAL SIGNATURES WORK

- ▶ Digital signature technology is defined in Florida Statutes 668, using one of several algorithms to encode a signer's personal information, making it possible to authenticate the signature using the Encryption key produces
- ▶ PDF management software such as Adobe Acrobat or BlueBeam can be used to decode the signature, authenticate the signature and read the history of the file to determine if the file has been changed since the document was signed

FLORIDA STATUTE 668

- ▶ As used in this act:
- ▶ (1) “Certificate” means a computer-based record which:
 - ▶ (a) Identifies the certification authority.
 - ▶ (b) Identifies the subscriber.
 - ▶ (c) Contains the subscriber’s public key.
 - ▶ (d) Is digitally signed by the certification authority.

FLORIDA STATUTE 668

- ▶ (2) "Certification authority" means a person who issues a certificate.
- ▶
- ▶ (3) "Digital signature" means a type of electronic signature that transforms a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine:
 - ▶ (a) Whether the transformation was created using the private key that corresponds to the signer's public key.
 - ▶ (b) Whether the initial message has been altered since the transformation was made.
- ▶ A "key pair" is a private key and its corresponding public key in an asymmetric cryptosystem, under which the public key verifies a digital signature the private key

FLORIDA STATUTE 668

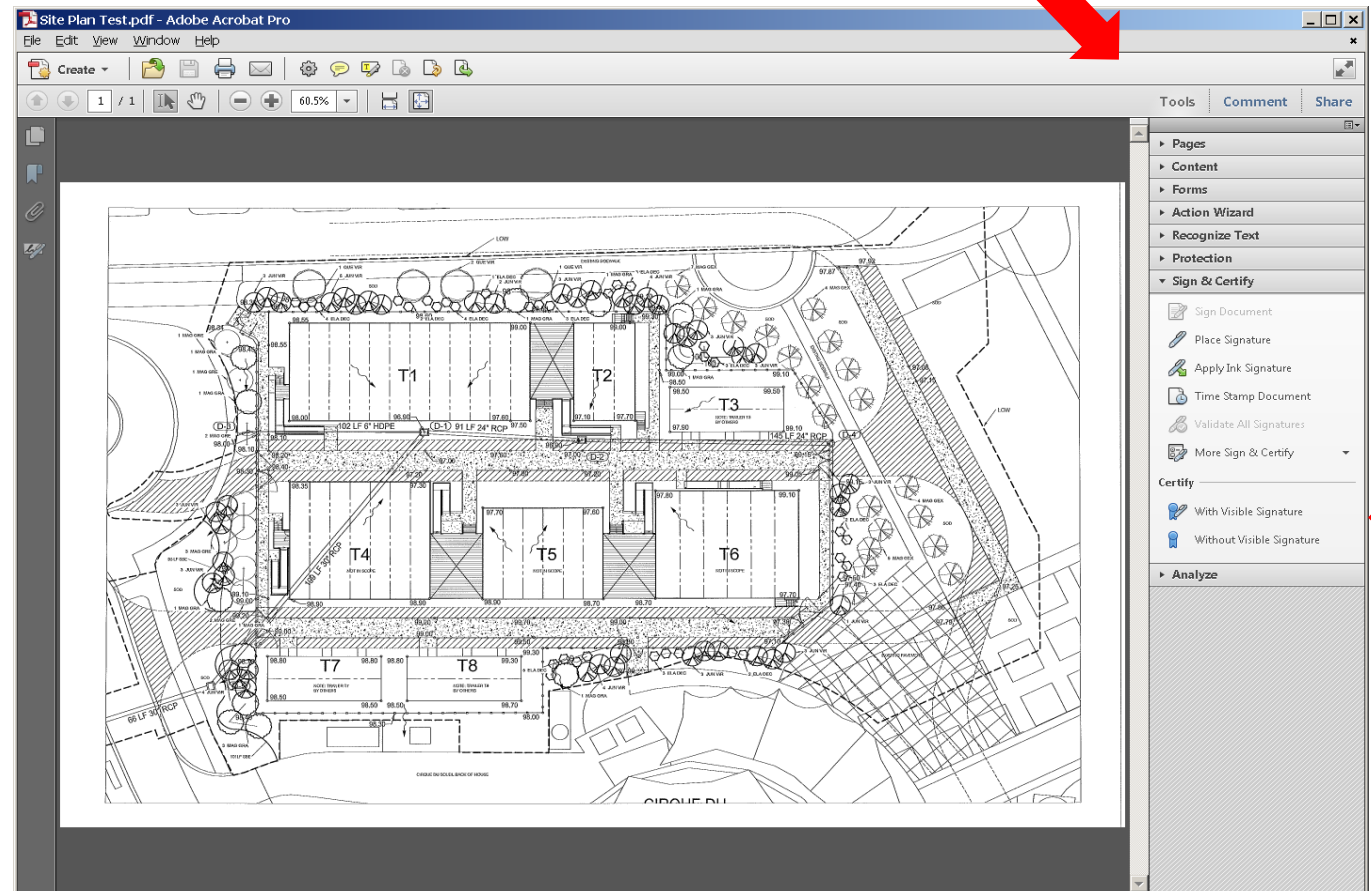
- ▶ (3) “Digital signature” means a type of electronic signature that transforms a message using an asymmetric cryptosystem such that a person having the initial message and the signer’s public key can accurately determine:
 - ▶ (a) Whether the transformation was created using the private key that corresponds to the signer’s public key.
 - ▶ (b) Whether the initial message has been altered since the transformation was made.

FLORIDA STATUTE 668

- ▶ A “key pair” is a private key and its corresponding public key in an asymmetric cryptosystem, under which the public key verifies a digital signature the private key creates. An “asymmetric cryptosystem” is an algorithm or series of algorithms which provide a secure key pair.

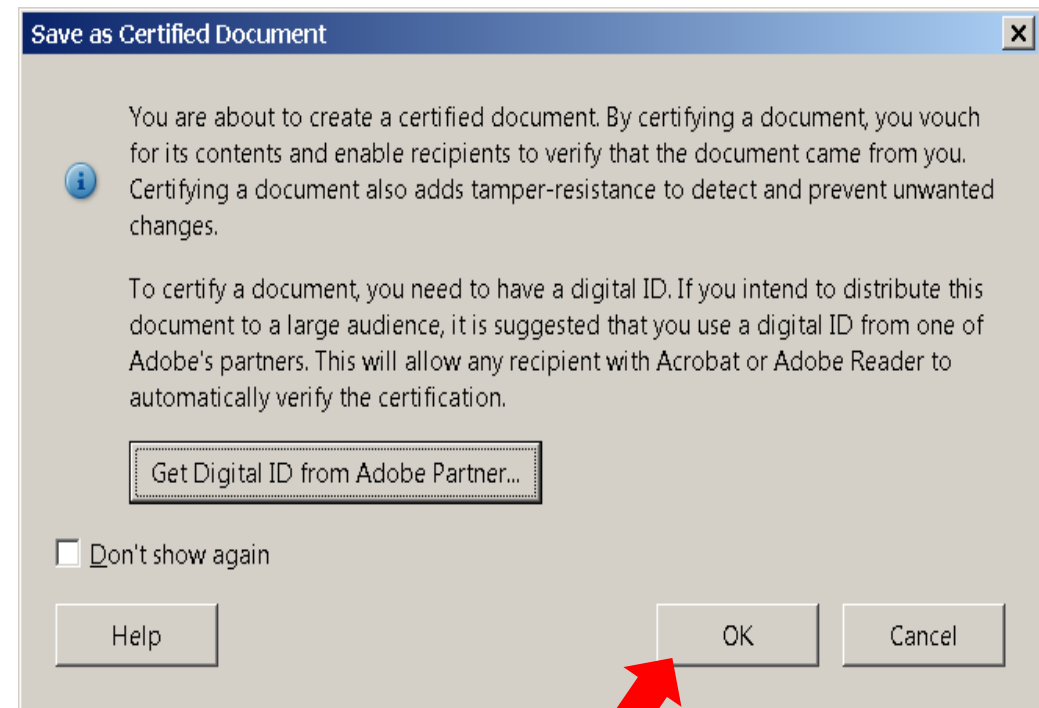
CREATING A SIGNATURE

- To create a digital signature, open the “Tools” panel and select “Visual Signature”



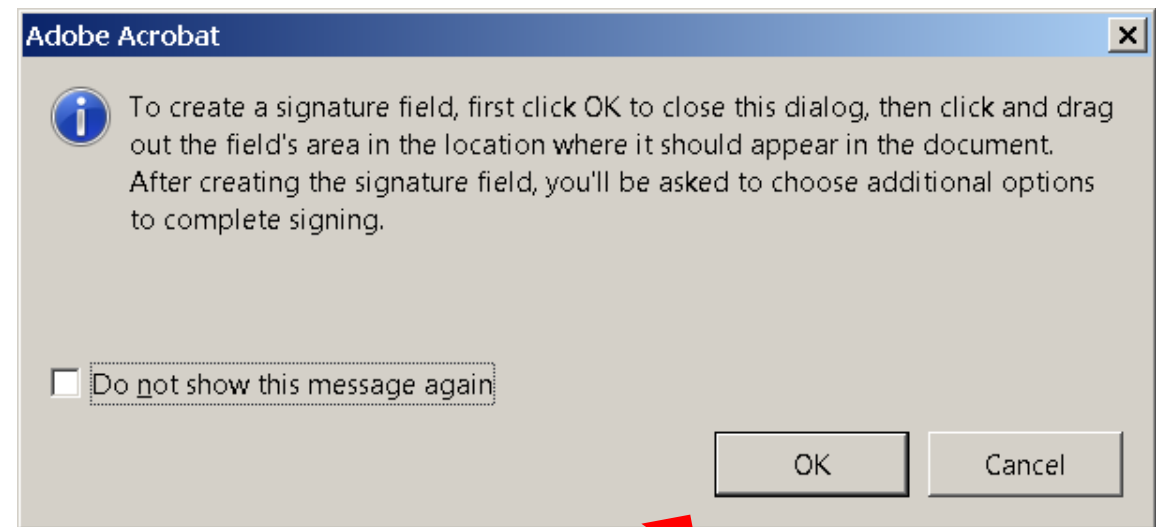
CREATING A SIGNATURE

Click on "OK" at the first screen



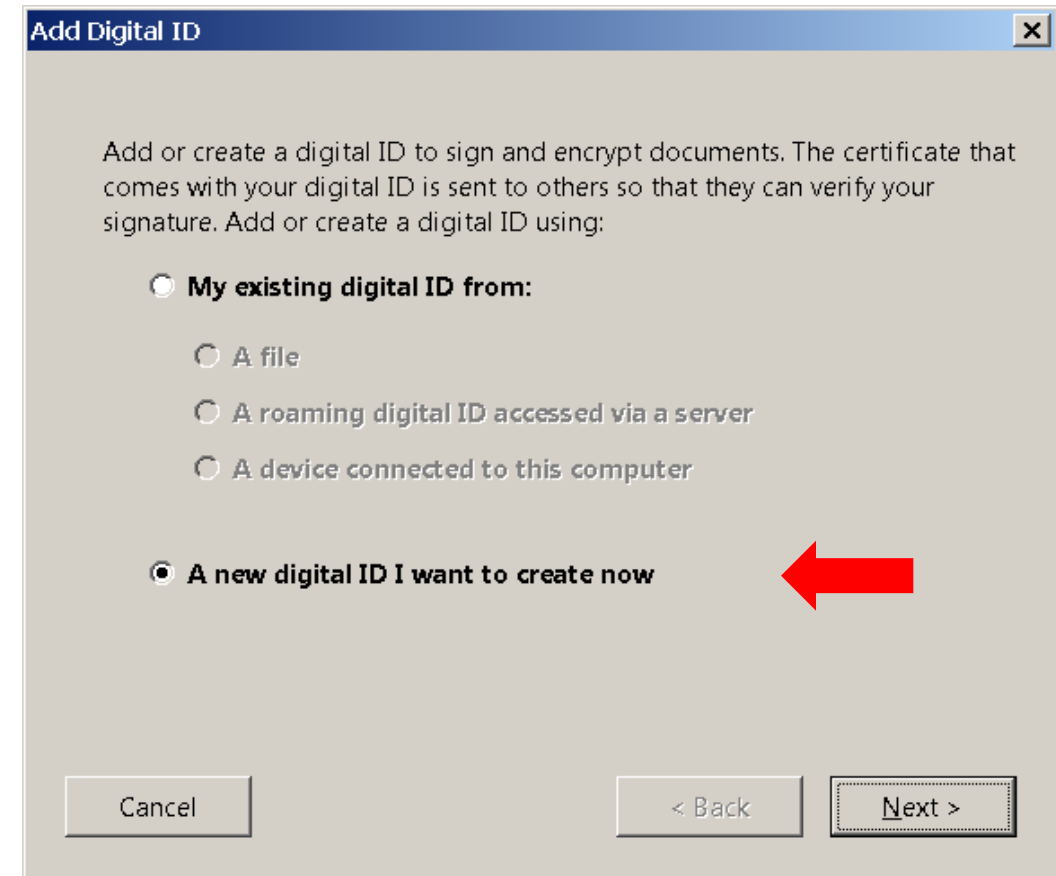
CREATE A SIGNATURE

- ▶ Click "OK" to create a signature field.



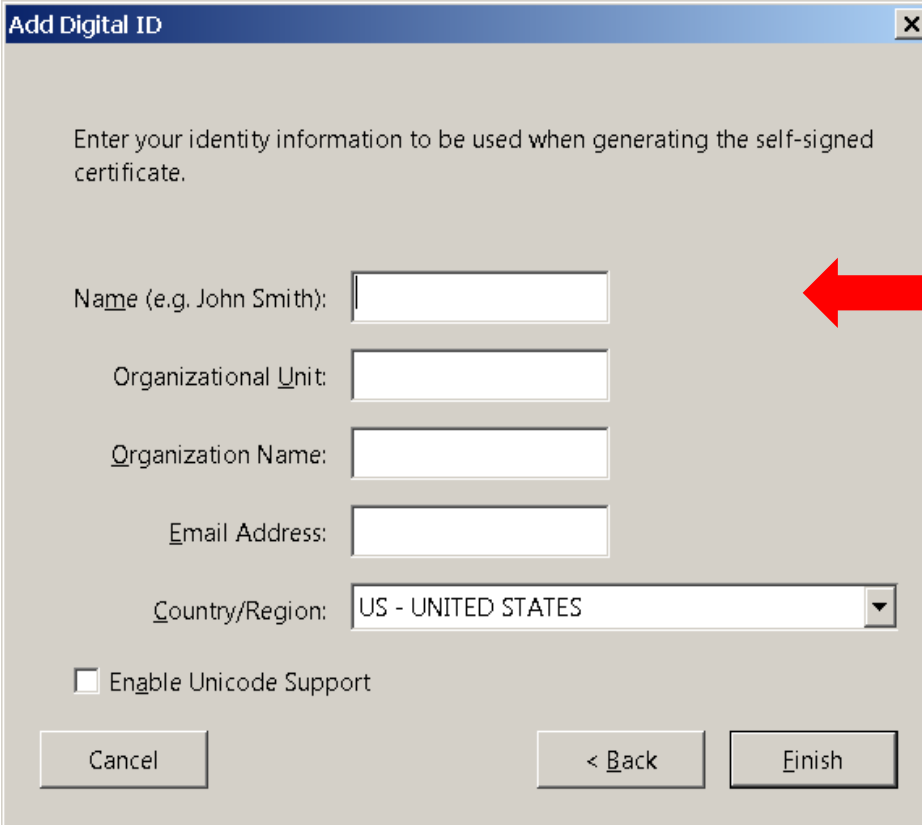
CREATING A SIGNATURE

- ▶ After the signature field is created the signature file can be selected, or a new signature can be created.
- ▶ Note that you only have to sign a signature file once
- ▶ Select "New Digital ID" to create your signature



CREATING A SIGNATURE

- Fill in all of the open fields and click "Finish"



The screenshot shows a Windows-style dialog box titled "Add Digital ID". Inside, there is a text prompt: "Enter your identity information to be used when generating the self-signed certificate." Below this are five input fields: "Name (e.g. John Smith):", "Organizational Unit:", "Organization Name:", "Email Address:", and "Country/Region:". The "Country/Region:" field is a dropdown menu currently showing "US - UNITED STATES". At the bottom, there is an unchecked checkbox labeled "Enable Unicode Support" and three buttons: "Cancel", "< Back", and "Finish". A prominent red arrow points from the right edge of the dialog box towards the "Name" input field, indicating where the user should enter their name.

Add Digital ID

Enter your identity information to be used when generating the self-signed certificate.

Name (e.g. John Smith):

Organizational Unit:

Organization Name:

Email Address:

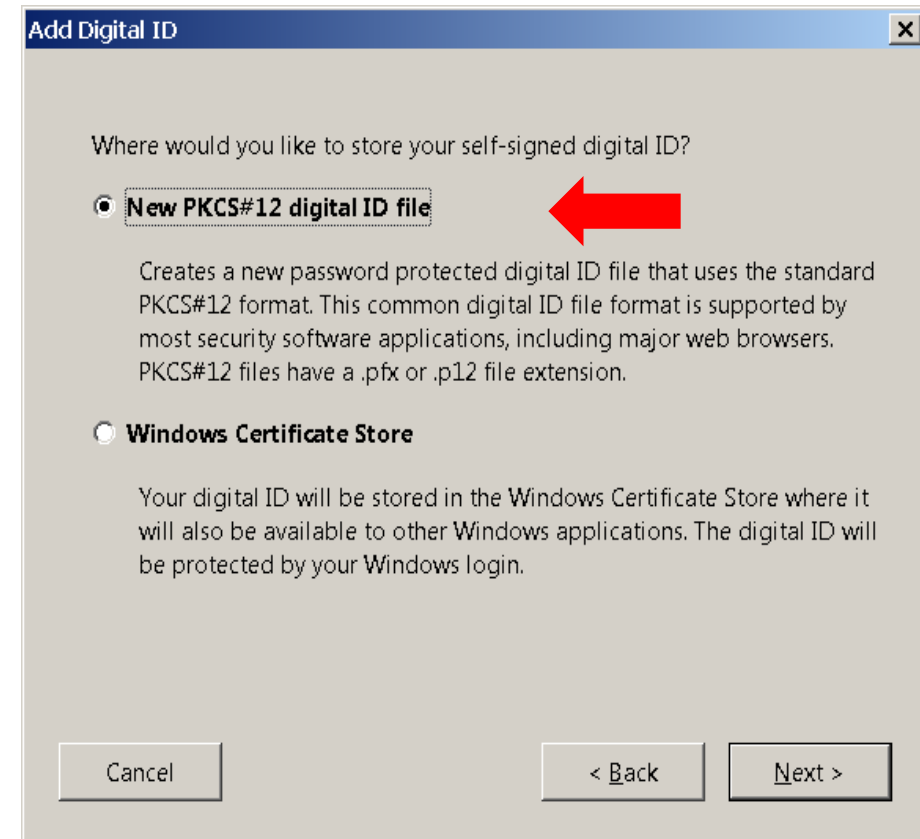
Country/Region:

☐ Enable Unicode Support

Cancel < Back Finish

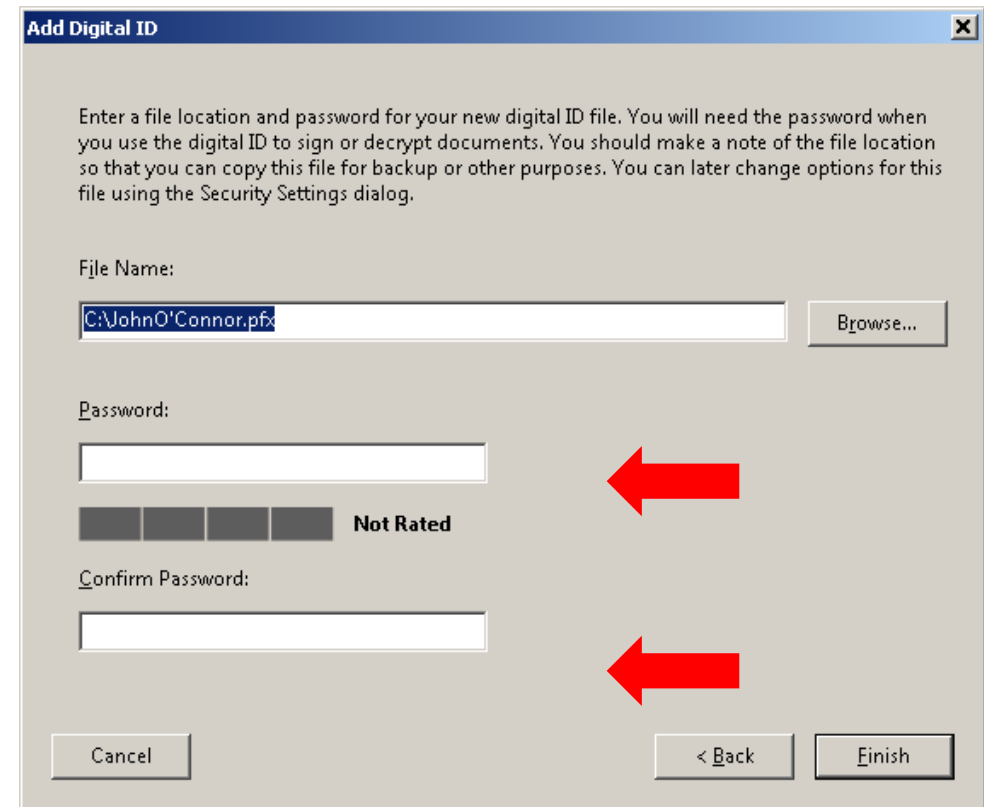
CREATING A SIGNATURE

- ▶ To create a password protected Digital ID select "New PKCS#12 digital ID File" and click Next



CREATING A SIGNATURE

- ▶ The file name will pre-load
- ▶ Create a password and confirm
- ▶ Click "Finish"



Add Digital ID

Enter a file location and password for your new digital ID file. You will need the password when you use the digital ID to sign or decrypt documents. You should make a note of the file location so that you can copy this file for backup or other purposes. You can later change options for this file using the Security Settings dialog.

File Name:

Password:

Not Rated

Confirm Password:

Two red arrows point to the password and confirm password input fields.

CREATING A SIGNATURE

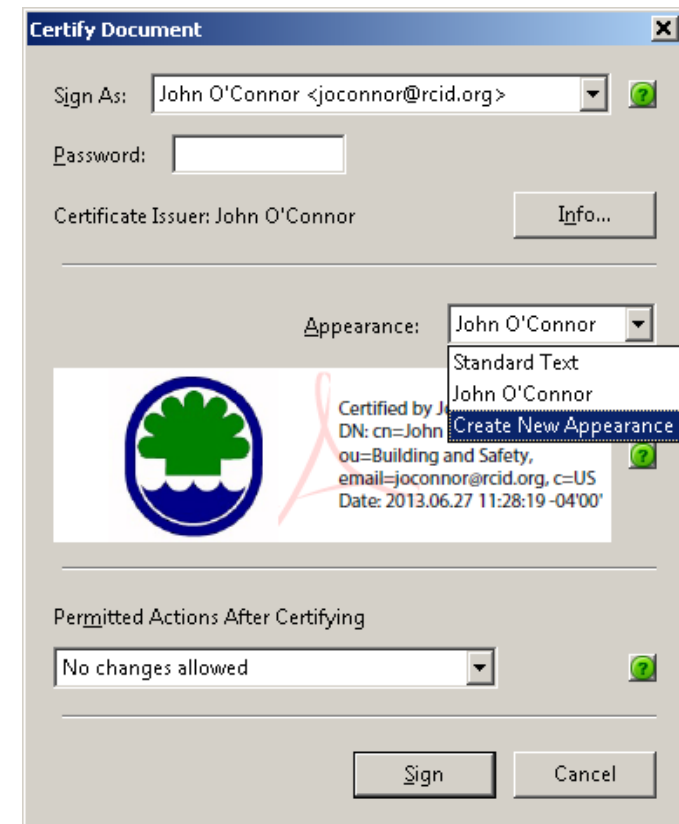
- ▶ Now your digital ID has been created and can be used to certify the document
- ▶ The top line is your signature file name; It will auto-load
- ▶ On the second line fill in your password
- ▶ The third line is the name of the visible signature, it will auto-load
- ▶ The fourth line will auto load the signature info

The screenshot shows the 'Certify Document' dialog box with the following fields and options:

- Sign As:** John O'Connor <joconnor@rcid.org> (indicated by a red arrow)
- Password:** (empty text box)
- Certificate Issuer:** John O'Connor (with an 'Info...' button)
- Appearance:** John O'Connor (indicated by a red arrow)
- Signature Preview:** A box containing a logo, a red signature, and the text: 'Certified by John O'Connor DN: cn=John O'Connor, o=RCID, ou=Building and Safety, email=joconnor@rcid.org, c=US Date: 2013.06.27 11:28:19 -04'00'' (indicated by a red arrow)
- Permitted Actions After Certifying:** A dropdown menu with the following options:
 - Annotations, form fill-in, and digital signatu
 - No changes allowed
 - Form fill-in and digital signatures
 - Annotations, form fill-in, and digital signatures (highlighted)(indicated by a red arrow)
- Buttons:** 'Cancel' and a help icon (?)

CREATING A SIGNATURE

- Open the drop-down list and select choose new Appearance



The screenshot shows the 'Certify Document' dialog box. The 'Sign As' field is set to 'John O'Connor <joconnor@rcid.org>'. The 'Password' field is empty. The 'Certificate Issuer' is 'John O'Connor'. The 'Appearance' dropdown menu is open, showing options: 'John O'Connor', 'Standard Text', and 'Create New Appearance...'. A red arrow points to the 'Create New Appearance...' option. Below the dropdown, there is a preview of the signature and a green question mark icon. The 'Permitted Actions After Certifying' dropdown is set to 'No changes allowed'. At the bottom are 'Sign' and 'Cancel' buttons.

Certify Document

Sign As: John O'Connor <joconnor@rcid.org> ?

Password:

Certificate Issuer: John O'Connor Info...

Appearance: John O'Connor ?

- Standard Text
- John O'Connor
- Create New Appearance...

Certified by John O'Connor
DN: cn=John O'Connor, ou=Building and Safety,
email=joconnor@rcid.org, c=US
Date: 2013.06.27 11:28:19 -04'00' ?

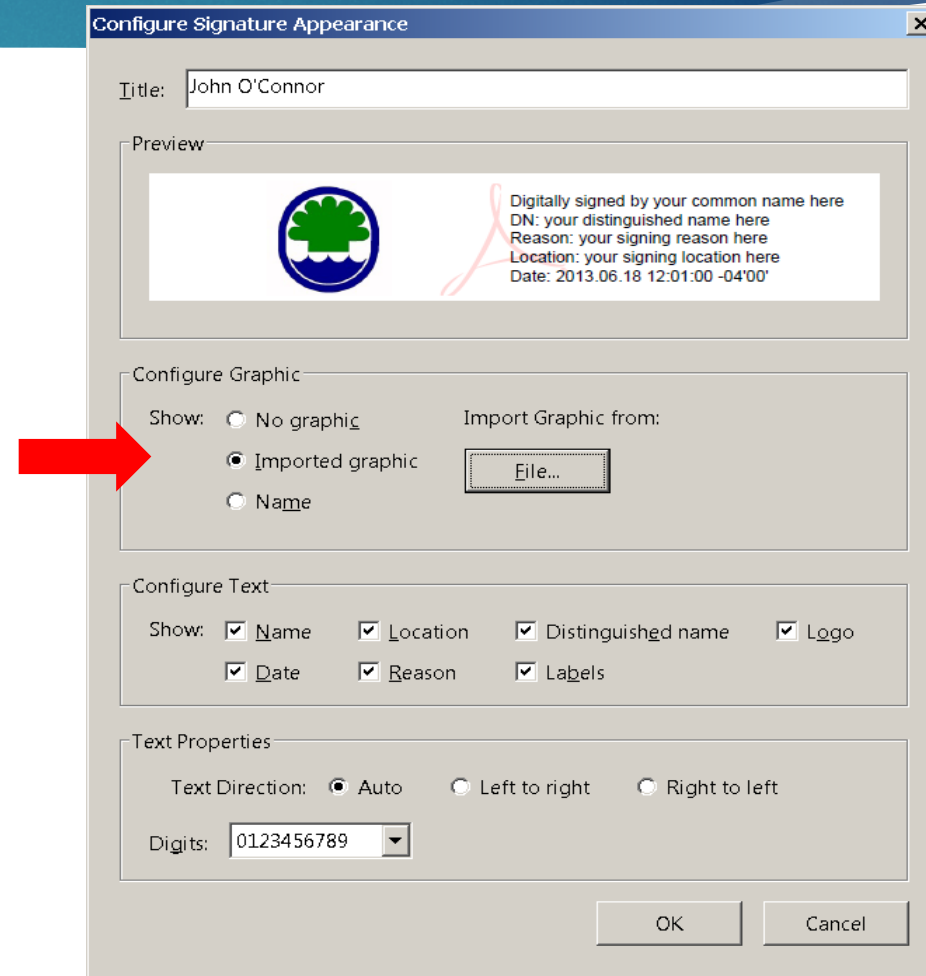
Permitted Actions After Certifying

No changes allowed ?

Sign Cancel

CREATING A SIGNATURE

- ▶ Name the signature
- ▶ Edit the fields as needed
- ▶ Import an image



The screenshot shows the 'Configure Signature Appearance' dialog box. A red arrow points to the 'Title' field, which contains 'John O'Connor'. Another red arrow points to the 'Imported graphic' radio button in the 'Configure Graphic' section. The 'Preview' section shows a digital signature with a green tree logo and text: 'Digitally signed by your common name here', 'DN: your distinguished name here', 'Reason: your signing reason here', 'Location: your signing location here', and 'Date: 2013.06.18 12:01:00 -04'00''. The 'Configure Text' section has checkboxes for 'Name', 'Location', 'Distinguished name', 'Logo', 'Date', 'Reason', and 'Labels', all of which are checked. The 'Text Properties' section has radio buttons for 'Text Direction' (Auto, Left to right, Right to left) and a 'Digits' dropdown menu set to '0123456789'. The 'OK' and 'Cancel' buttons are at the bottom right.

Configure Signature Appearance

Title: John O'Connor

Preview

Digitally signed by your common name here
DN: your distinguished name here
Reason: your signing reason here
Location: your signing location here
Date: 2013.06.18 12:01:00 -04'00'

Configure Graphic

Show: ☐ No graphic ☒ Imported graphic ☐ Name

Import Graphic from: File...

Configure Text

Show: ☒ Name ☒ Location ☒ Distinguished name ☒ Logo
☒ Date ☒ Reason ☒ Labels

Text Properties

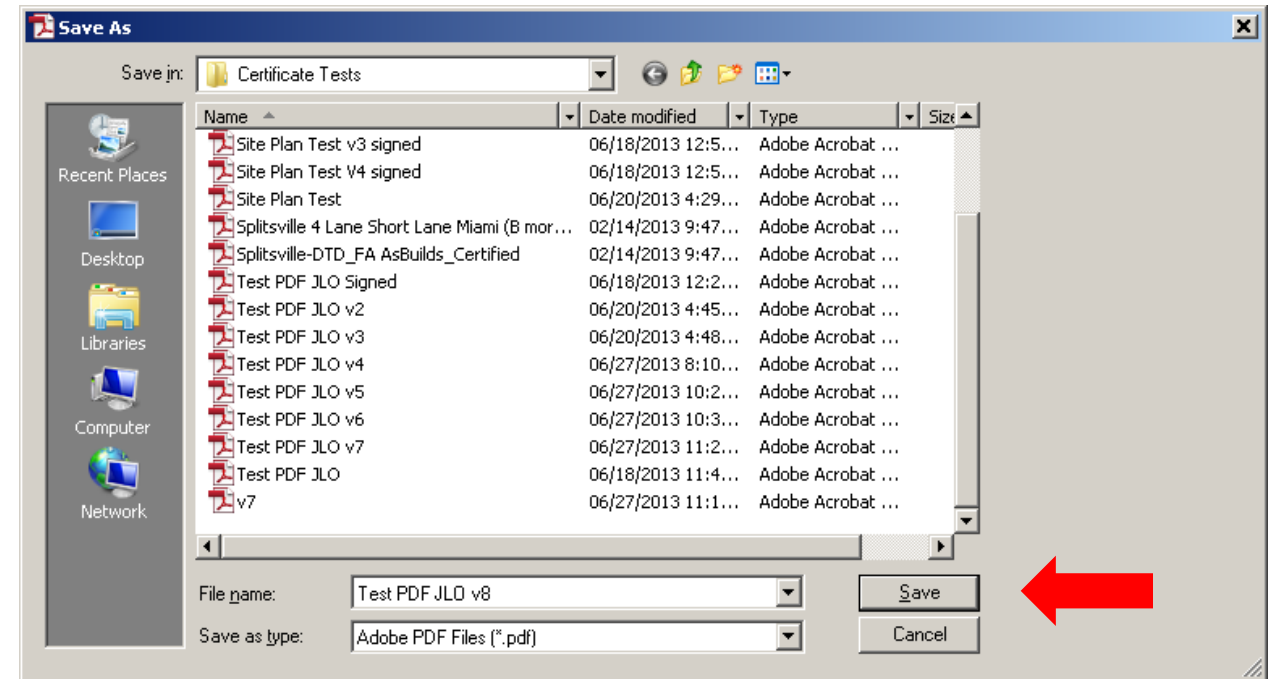
Text Direction: ☒ Auto ☐ Left to right ☐ Right to left

Digits: 0123456789

OK Cancel

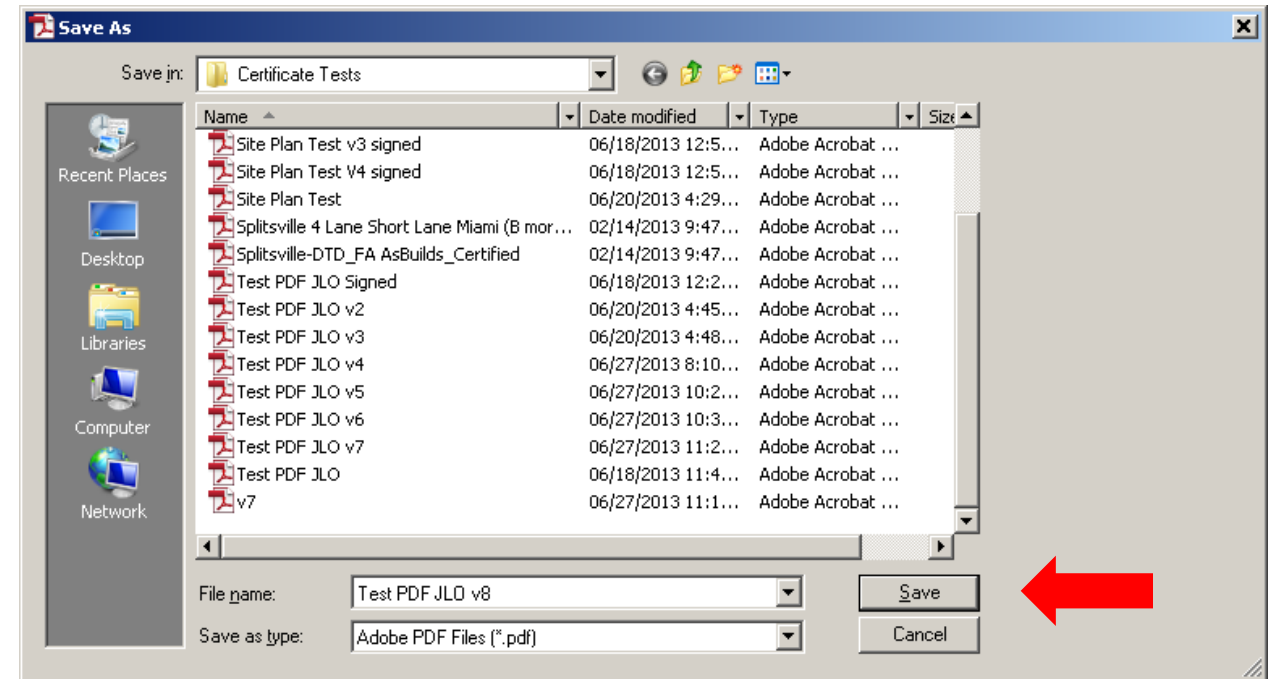
CREATING A SIGNATURE

- Before the signature is added the file must be saved



CREATING A SIGNATURE

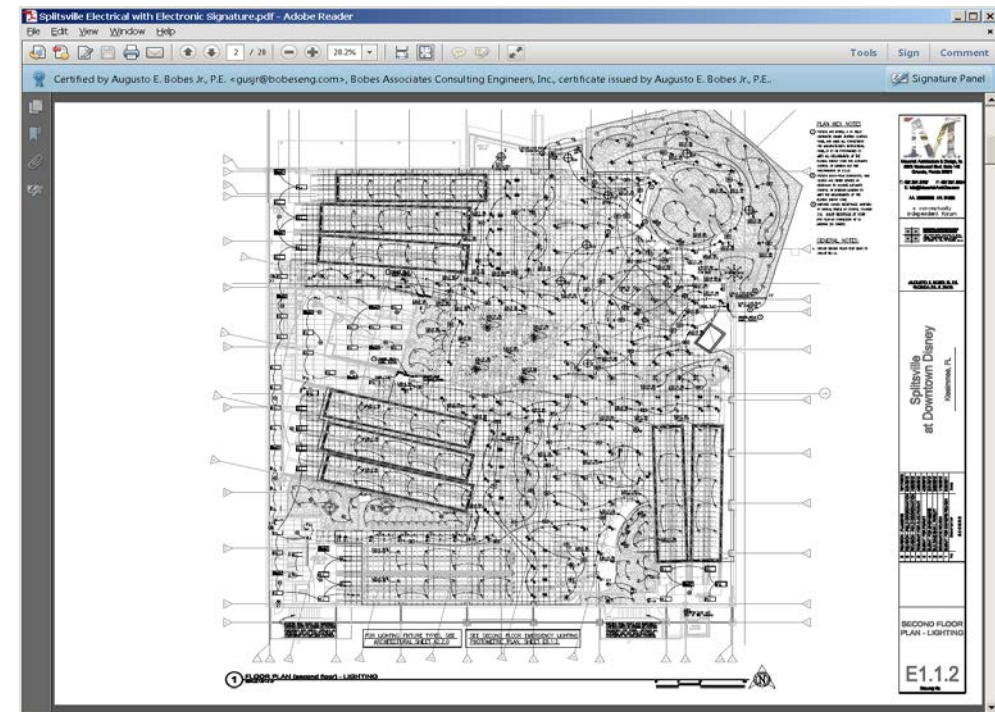
- Before the signature is added the file must be saved



VALIDATING A SIGNATURE

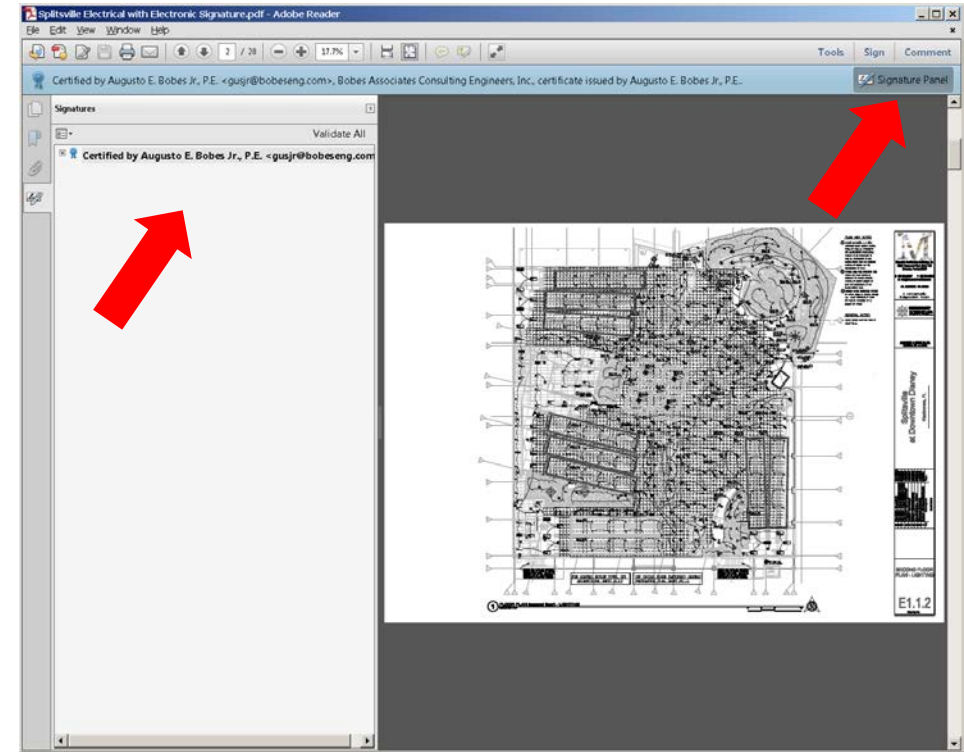
The most commonly used PDF reader is ADOBE Arobat. With their free PDF reader it is possible to view file content, see the document history and validate digital signatures

When a drawing file is opened with Adobe Acrobat, the program will indicate if it has been digitally signed by showing the signature panel button in the right side of the tray above the drawing



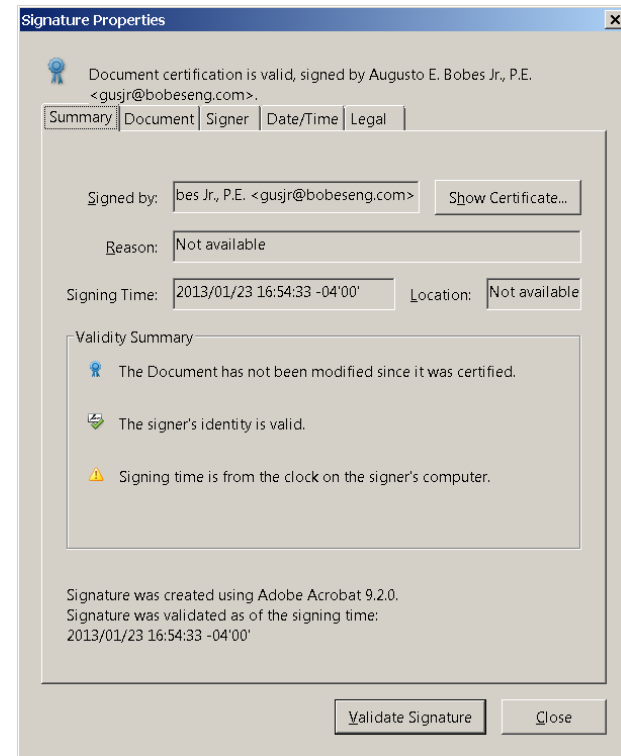
VALIDATING A SIGNATURE

- ▶ Click on the Signature Panel button to open the signature panel
- ▶ The name of the signee will be shown



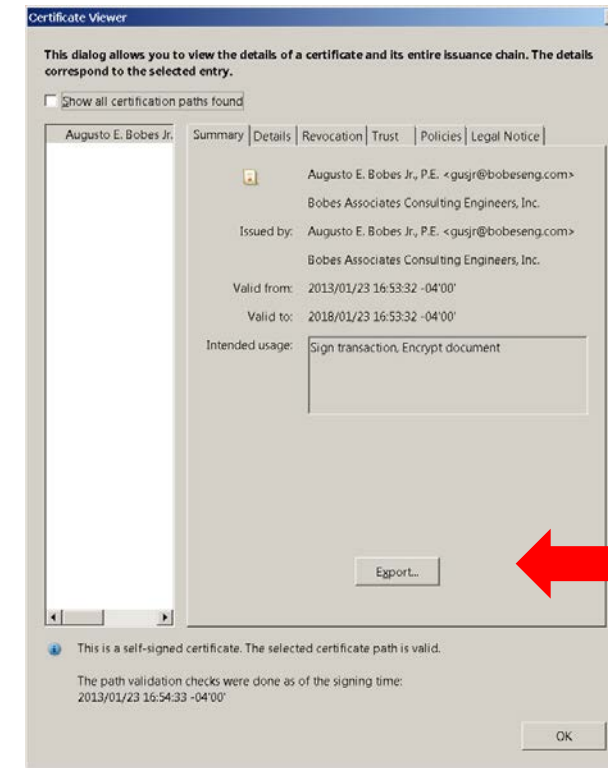
VALIDATING A SIGNATURE

- ▶ From the Signature Properties panel click on the Show Certificate button



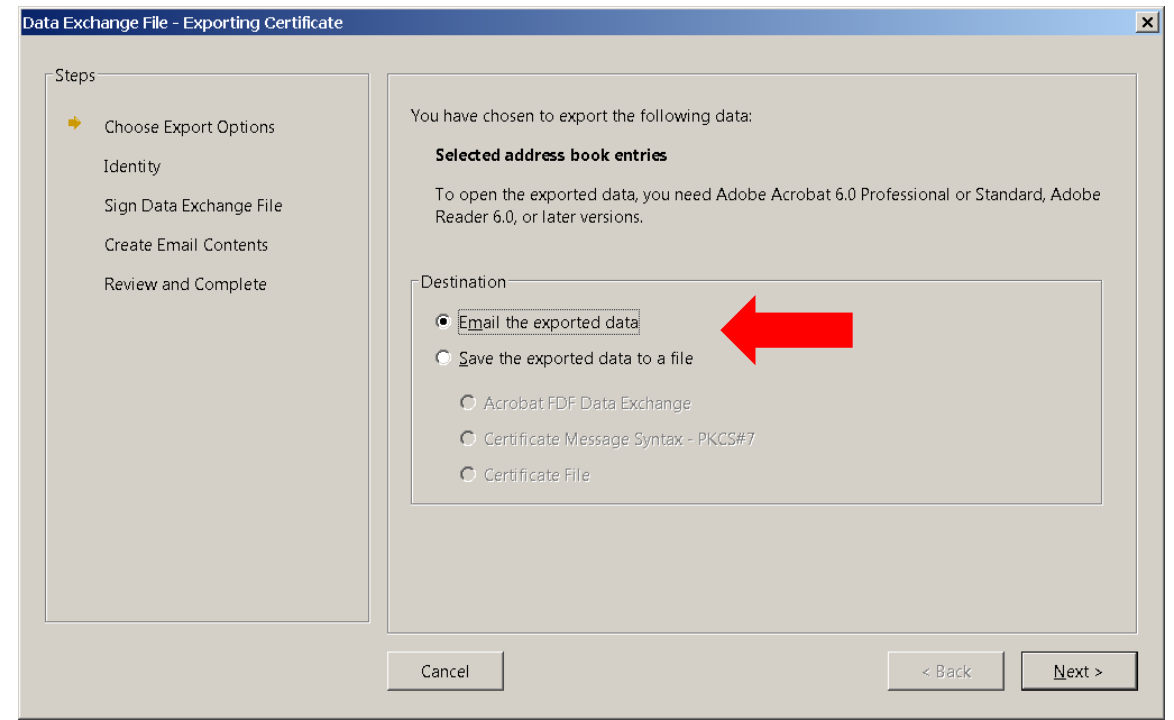
EXPORTING A PUBLIC KEY

- ▶ The signee must send the public key to the Authority Having Jurisdiction
- ▶ This is done by exporting the public key
- ▶ The Authority Having Jurisdiction must receive the public key and save it in the adobe trusted certificate folder



EXPORTING A PUBLIC KEY

- ▶ Click on the Export the encrypted data line and then the next button



EXPORTING A PUBLIC KEY

- Fill in the information and click the next button

Data Exchange File - Exporting Certificate

Steps

- Choose Export Options
- Identity**
- Sign Data Exchange File
- Create Email Contents
- Review and Complete

Your identity information is used with comments, reviews, and digital signatures. Information entered here is secure and not transmitted beyond this application without your knowledge. To modify this information in the future, simply go to the Identity panel in the preferences.

Identity

Login Name: o'connorj

Name:

Title:

Organization Name:

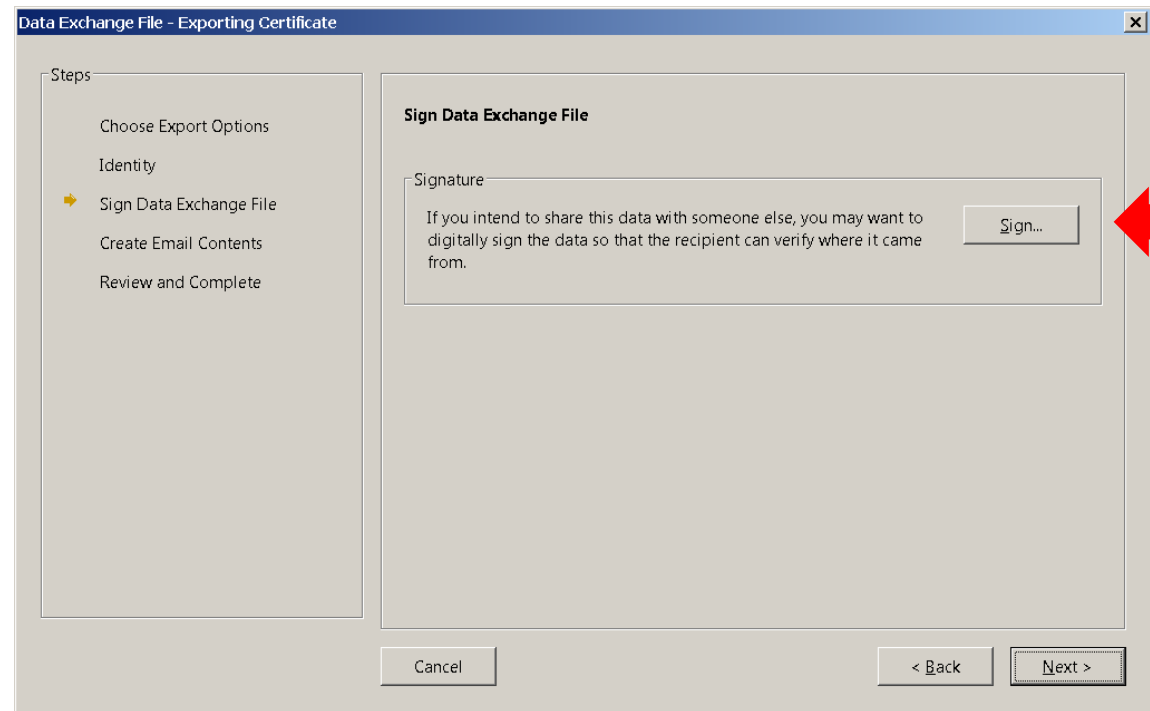
Organization Unit:

Email Address:

☐ Do not show again

EXPORTING A PUBLIC KEY

- ▶ Skip the sign the file option and click next



EXPORTING A PUBLIC KEY

- ▶ Address the file to the Authority Having Jurisdiction and click next

Data Exchange File - Exporting Certificate

Steps

- Choose Export Options
- Identity
- Sign Data Exchange File
- ➔ Create Email Contents
- Review and Complete

You can specify the contents of the email message to which you will attach the exported data. This information will be sent to your email program.

Message

To:

Subject: Acrobat FDF Data Exchange File

Attached is an Acrobat FDF Data Exchange File.

The attached file contains a list of certificates that you can use to validate signatures and encrypt documents.

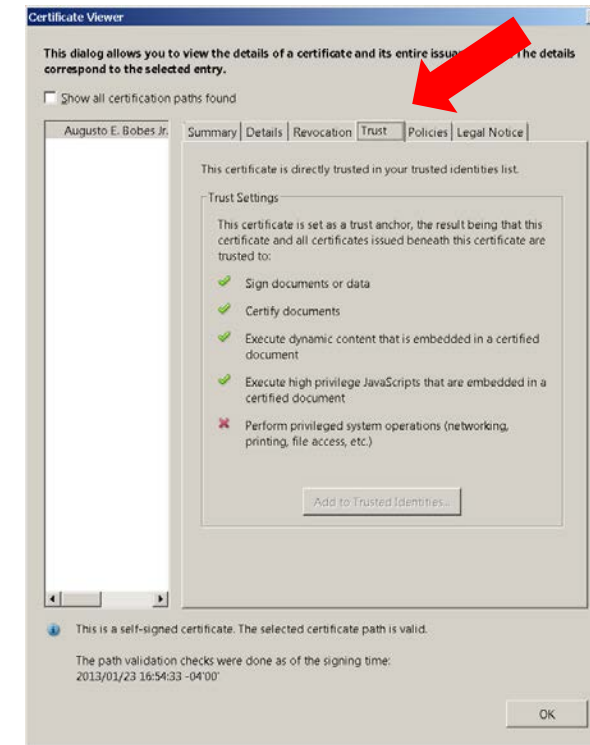
Opening this file will start Adobe Acrobat or Adobe Reader and prompt you to process the file.

To open and process the file attachment, you need Adobe Acrobat 6.0 Professional or Standard, Adobe Reader 6.0, or later versions.

Cancel < Back Next >

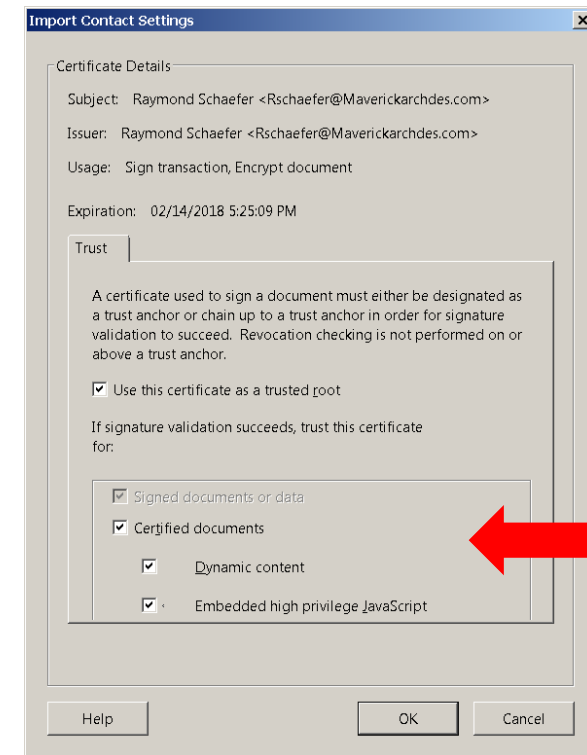
TRUSTING A CERTIFICATE

- ▶ Select the Trust tab and check all of the trust settings
- ▶ Click on the trust button



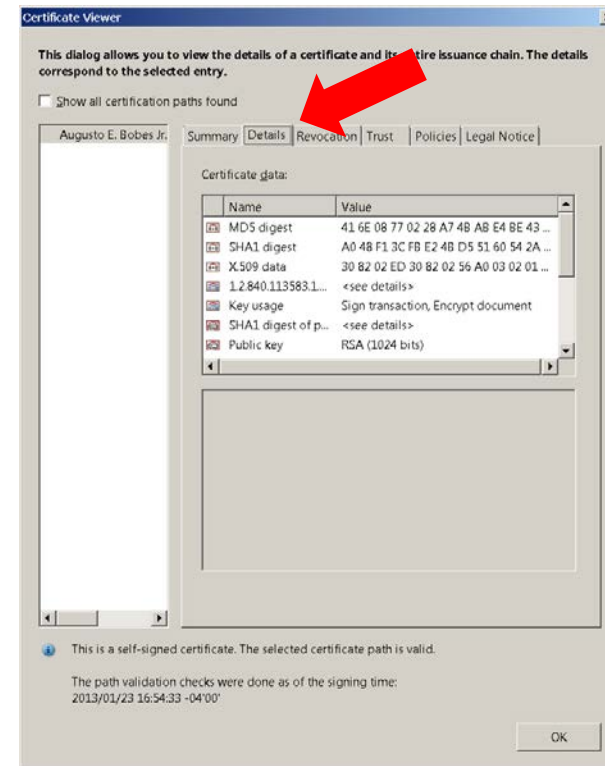
TRUSTING A CERTIFICATE

- ▶ Check the content boxes
- ▶ Click on the Ok button



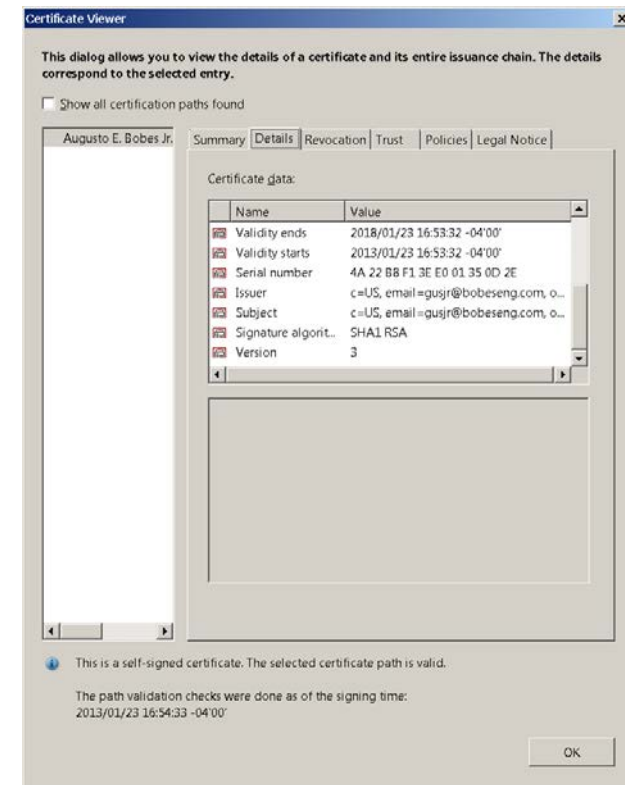
VIEWING SIGNATURE DETAILS

- Open the Details tab to view information about the signature



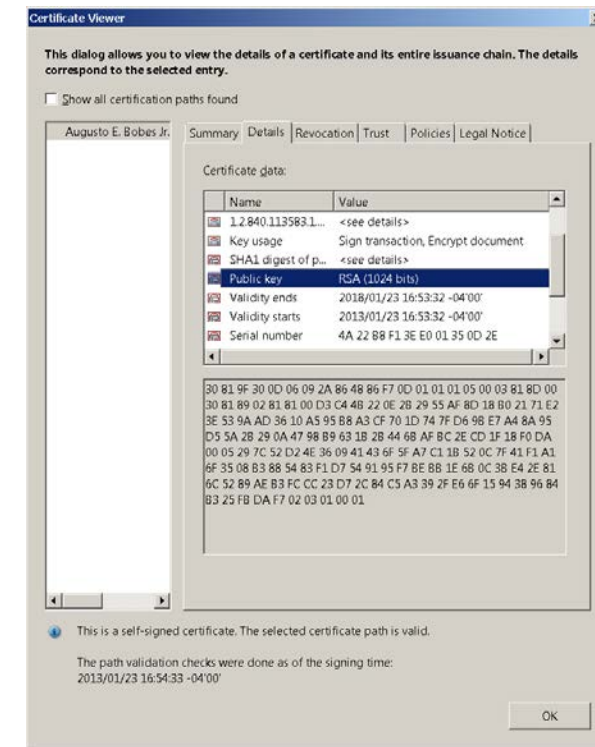
VIEWING SIGNATURE DETAILS

- Move the slide down to view more information



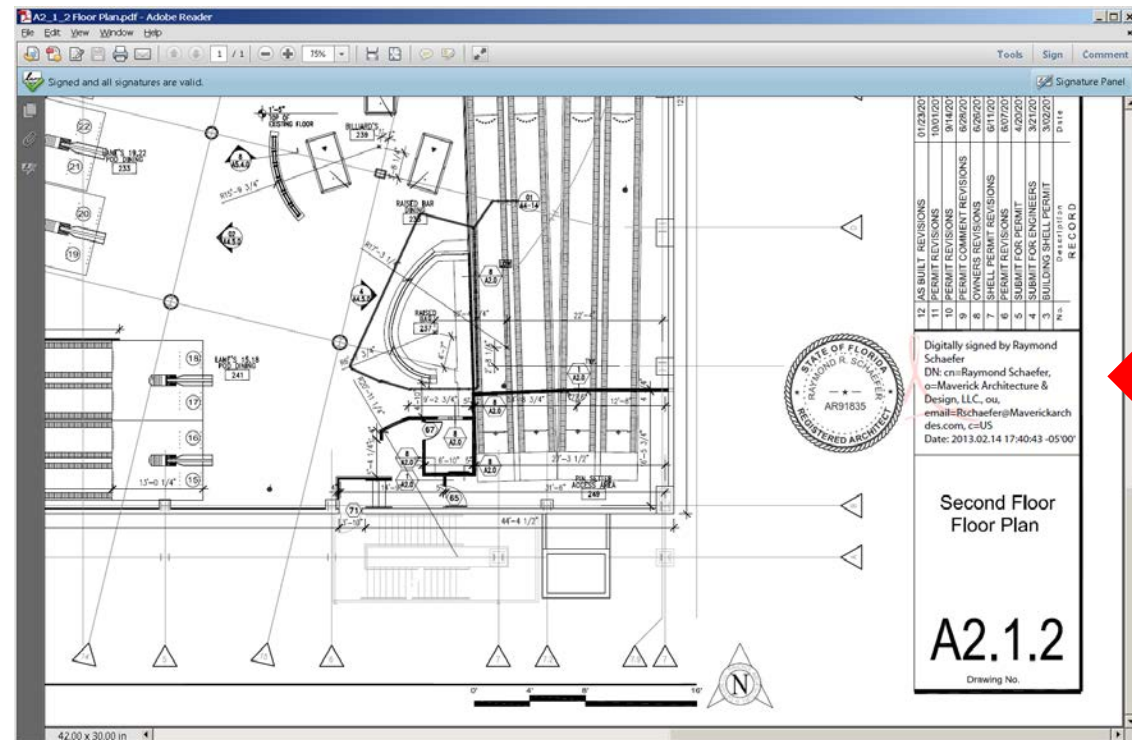
VIEWING SIGNATURE DETAILS

- The public key can be seen by highlighting the Public Key line



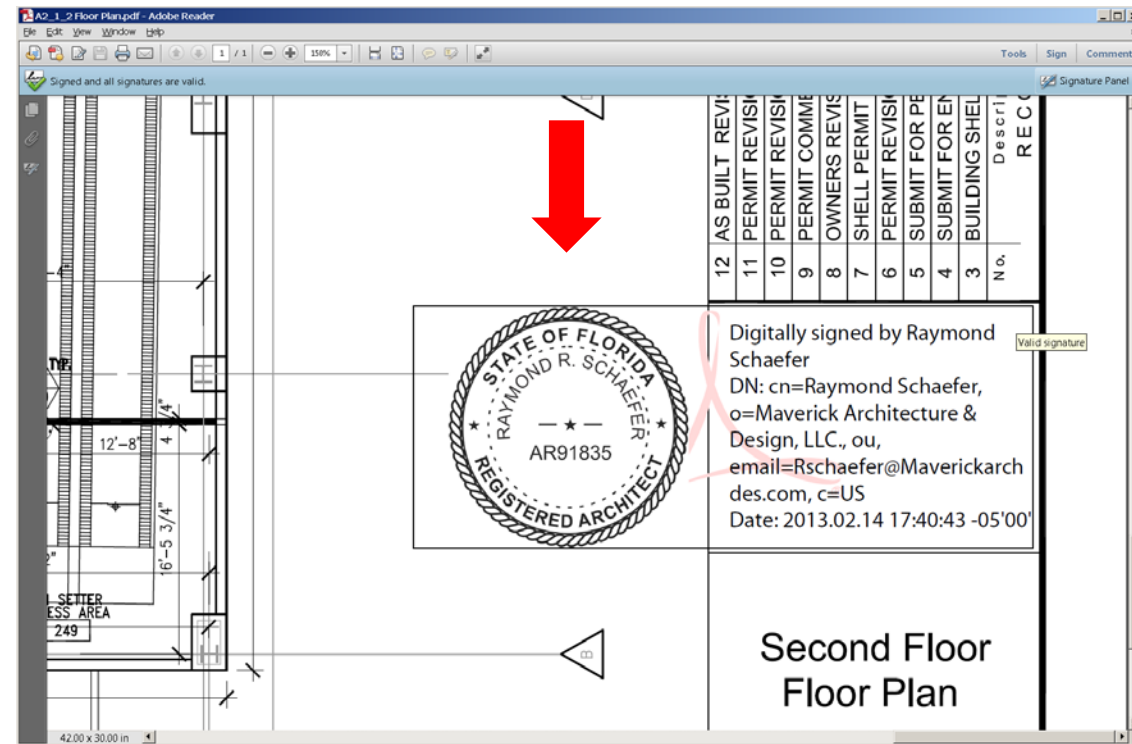
VISIBLE SIGNATURE IMAGES

- ▶ A visible signature image is not required in the validation process
- ▶ However, a visible signature image created by the signature software is helpful to notify the reviewer that the document is digitally signed
- ▶ A visible signature will contain information required by the rules



VISIBLE SIGNATURE IMAGES

- ▶ A proper visible image can include an image of the signee's seal, the name of the signee, date, contact information, and the phrase "Digitally signed by..."



THANK YOU FOR ATTENDING

